White Paper

Forescout Platform Orchestration Use Cases for IT Service Management (ITSM) Solutions

Table of Contents

State of ITSM Solutions 3

The Forescout Platform Is Foundational 4

The Forescout Platform for ITSM Use Cases 4

Real-Time Asset Intelligence 4

Workflow 5

Asset Lifecycle Management 5

Onboarding 6

Deploying 6

Maintaining 6

Retiring 6

Automation of MAR for IoT Authentications 7

Workflow 7

Use CMDB as the Verification Source for Authentications 8

Workflow 8

Increase Service Desk Efficiency 8

Workflow 8

Optimize Security Operations 9

Workflow 9

Security Compliance 9

Workflow 10

Out of the box integration with ServiceNow 10

The Forescout Platform and Other ITSM Solutions 11

Product Requirements 12

State of ITSM Solutions

IT Service Management (ITSM) solutions are only as good as the accuracy and relevancy of the asset data upon which they rely. ITSM vendors' discovery solutions historically have been focused on the data center, associated devices, infrastructure components and their relationships to each other. They are not intended to provide complete, continuous visibility of network-connected campus, data center, cloud, virtual, IoT, mobile (transient and BYOD) and OT assets. ITSM discovery solutions typically perform scheduled scans, which means that the data contained within the Configuration Management Database (CMDB), which is the underlying system of record for ITSM solutions remains static for long periods of time and is usually updated only when subsequent scans occur. This is problematic in dynamic environments where changes may occur often. As the CMDB is supposed to represent the expected state of the environment at any given point in time, it should be up to date. Also, when there are deviations from what is contained in the CMDB, even though they may be valid changes, someone should investigate and ensure they are in fact valid and that there are change requests in the ITSM system to account for them. So, the question becomes, how do I ensure that my CMDB is accurate and complete at all times?

Organizations typically have multiple discovery sources for obtaining data about the various devices and network components in their environments. Patching solutions like Microsoft SCCM[1] or IBM BigFix, vulnerability scanning products such as those from Tenable or Qualys, endpoint protection platforms like Symantec or CrowdStrike and network/systems and fault management platforms like SolarWinds all discover devices based on their network scans, deployed agents or the SNMP[2] traps sent to them. Figure 1 represents a typical discovery data process that is partial and incomplete due to issues such as broken agents, scans missing transient devices or fault management solutions that rely upon SNMP polling or traps. Each approach inherently has gaps in visibility; therefore, only a partial picture of the enterprise makes it into the CMDB.

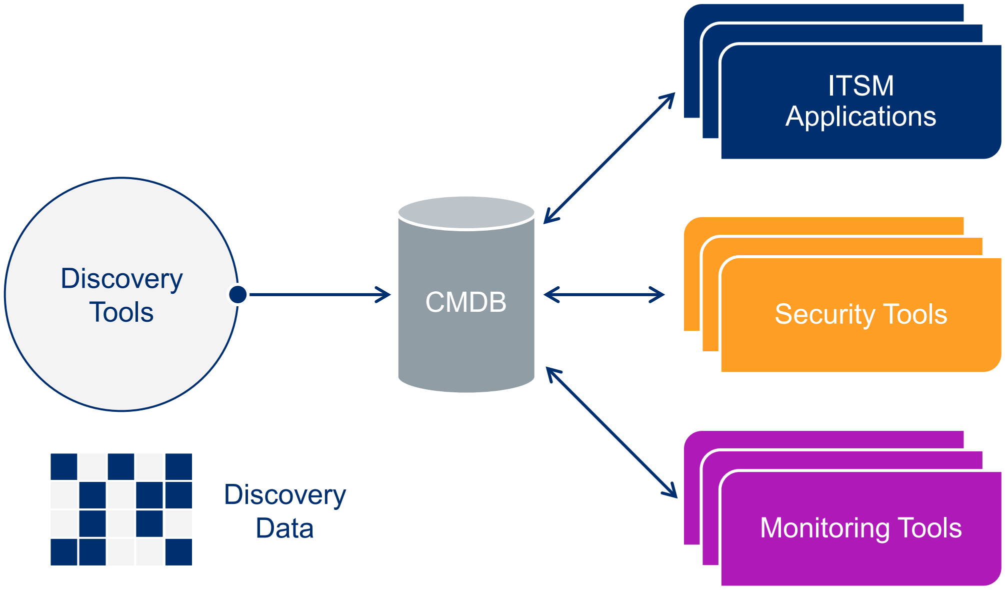


Figure 1: Often discovery solutions only provide partial data, which affects the accuracy and efficacy of systems down the line.

The Forescout Platform is Foundational

In light of the serious issues related to asset discovery that so many organizations face today, the justification for adopting the Forescout platform becomes abundantly clear. The device data the Forescout platform manages is continuously updated and at any given point in time provides a complete "as-is" representation of assets across the extended network environments. This real-time data accuracy is foundational to the CMDB and provides the basis upon which all ITSM processes rely.

For this reason, the Forescout platform should be deployed in order to obtain complete asset visibility as quickly as possible while gaining key cybersecurity protections in addition to supporting ITSM use cases. The Forescout platform can provide the initial loading of the data into the CMDB or, if there is already some data populated into the CMDB, the Forescout platform can augment that data.

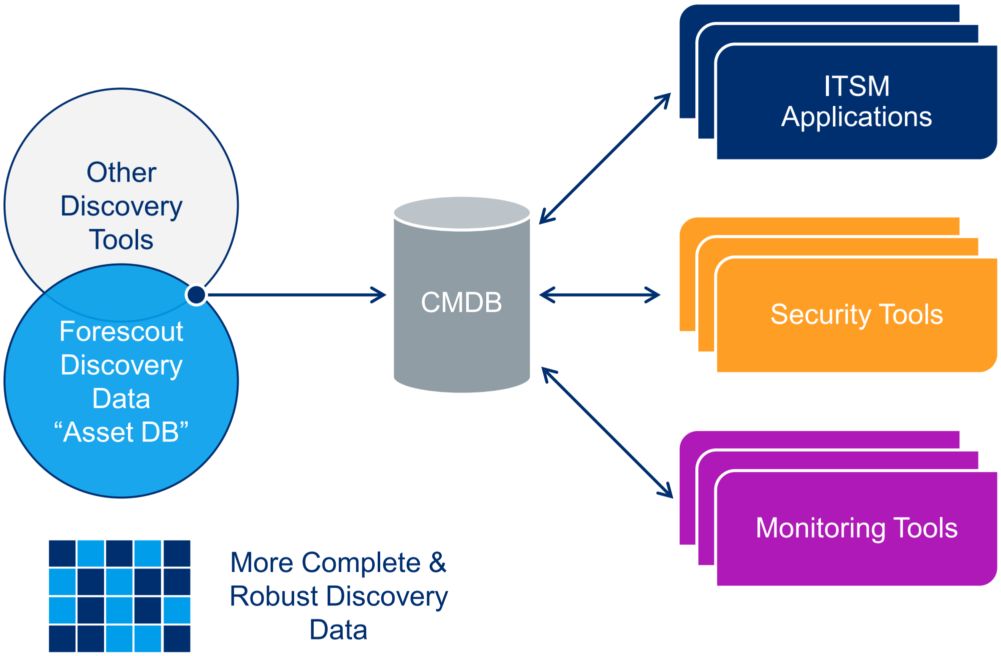

Other Discovery Tools
Forescout Discovery Data "Asset DB"
CMDB
ITSM Applications
Security Tools
Monitoring Tools
More Complete & Robust Discovery Data

Figure 2: Since the Forescout platform offers complete device visibility, it can provide the CMDB with the foundational data, and other systems can augment it.

The Forescout Platform for ITSM Use Cases

Integrating the Forescout platform into ITSM solutions helps to ensure the CMDB is populated with the most current status of all assets and configuration items in the environment. Unquestionably, multiple use cases are improved by a more accurate and complete CMDB, as outlined below.

Real-Time Asset Intelligence

The continuous monitoring function of the Forescout platform can play the role of an "auditor" and help equalize and bring both the Forescout platform and the ITSM system up to date. The Forescout platform enriches asset attributes with additional context, such as the switch port to which the device is connected, VLAN[3] information, network segment information, location, compliance status, and so on. It monitors and updates information in the asset inventory from the time a device enters the network until it leaves the network. The result is real-time asset monitoring and management that reduces the effort required to monitor and manage the assets and helps increase overall asset audit and security compliance.

Workflow

1. A device's information consisting of more than 100 properties is captured by the Forescout platform in real time when a device connects to the network.
2. The Forescout platform obtains the device's information from the ITSM platform, identifies discrepancies, and helps the ITSM platform update its repository.
3. The Forescout platform can also verify that the device has the latest patches; if not, it can inform the ITSM platform and trigger remediation actions.
4. Depending on the configuration, additional remediation actions may be taken. For example, a software update is pushed out from the ITSM platform and CMDB information is updated. The Forescout platform scans and finds that the device did not apply the update. The Forescout platform informs the ITSM platform and a different pre-defined workflow is initiated, which updates or reissues the software update based on the Forescout platform policy.

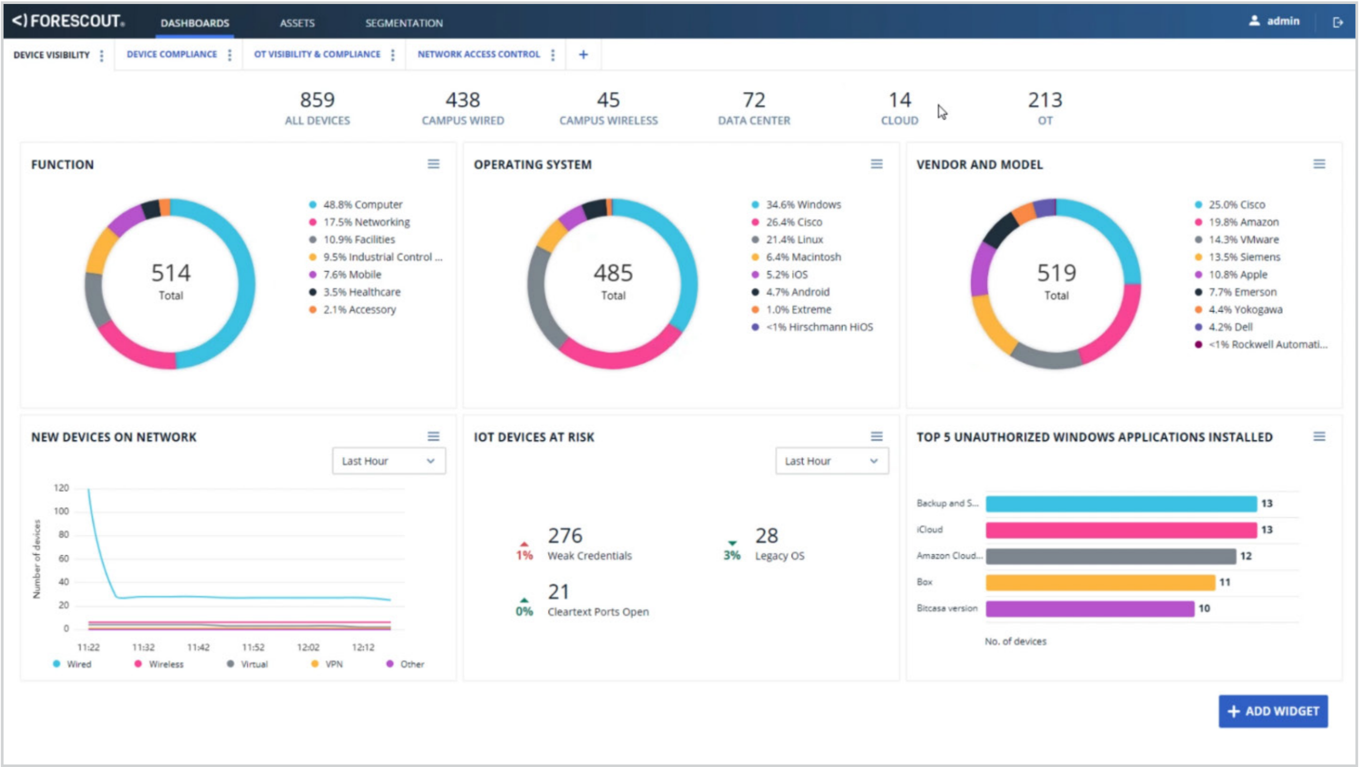


Figure 3: The Forescout platform provides real-time asset intelligence, and its continuous monitoring capability keeps both Forescout platform and the ITSM system up to date.

Asset Lifecycle Management

While effective asset lifecycle management involves many steps, many of the steps rely upon continual awareness of the state of the physical assets throughout their logical life. After the financial and contractual aspects of requesting and ordering of devices, the moment of onboarding is where the Forescout platform and its device visibility, contextual awareness and intelligent network access controls come into play. However, there are additional areas where the integration of the Forescout platform into an ITSM solution can bring significant value in security, network and operational settings. A high-level overview of an asset management process with associated descriptions of what and where the Forescout platform can provide help is documented below.

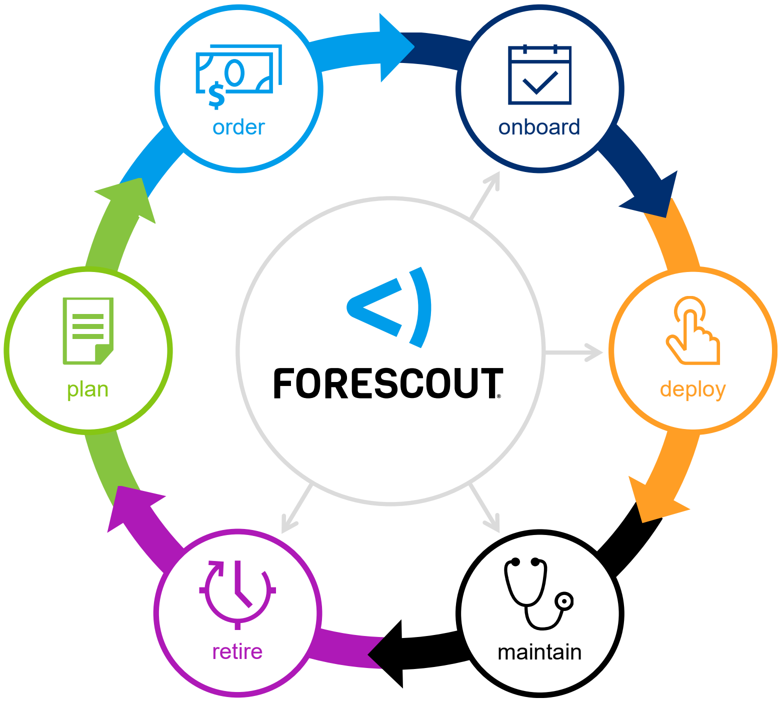


Figure 4: The Forescout platform impacts and improves key aspects of asset lifecycle management.

Onboarding

Independent of the Forescout platform, onboarding is the process that includes receiving and verifying the bill of lading as well as beginning the configuration process. Assets are unpacked and configured with the customer's baseline (if not performed by manufacturer) and are prepared for use in the enterprise. They are then tagged with an asset code and entered into the CMDB for tracking purposes. There is a true-up of the configuration of the asset in the CMDB while the imaging, installation and configuration processes take place. When placed onto the corporate network, the Forescout platform ensures standardization and compliance using pre-connect functions on a separate staging network.

Deploying

Now the asset is ready for distribution, which is indicated by a lifecycle status change in the CMDB. Once deployed into the field, the device's security posture is assessed to ensure compliance with the established security and regulatory policies. If needed, the Forescout platform updates the device's network assignment and any associated segmentation policies. In 802.1X[4] deployments, the Forescout platform and ITSM solutions automate this step with pre-population of the MAC Authentication Bypass Repository (MAR). In non-802.1X deployments, the Forescout platform can perform authentication via validating device status in the CMDB. Finally, the Forescout platform can update CMDB data to match real-time status of the asset.

Maintaining

During the normal course of service desk events, assets are updated in the CMDB by the Forescout platform as they are changed or moved. Any associated status or functional changes performed in the ITSM or CMDB regarding the device can trigger segmentation policy changes. The Forescout platform continuously checks for compliance and updates the CMDB as needed based on corporate policy. Any identified issues are addressed and/or recorded in an incident in order to maintain end-to-end tracking, which improves communication across the organization by sharing real-time data through centralized platforms.

Retiring

When devices are ready to be retired based on costs of maintenance, contract expiration, etc., the ITSM/ITSM lifecycle status changes. By leveraging that lifecycle status, the Forescout platform can control access to the network and associated resources. In the case of a retired device, the device will not be permitted on the network. In cases where a MAR or ITSM environment is leveraged for network authentications, the Forescout platform will disallow network access for retired assets.

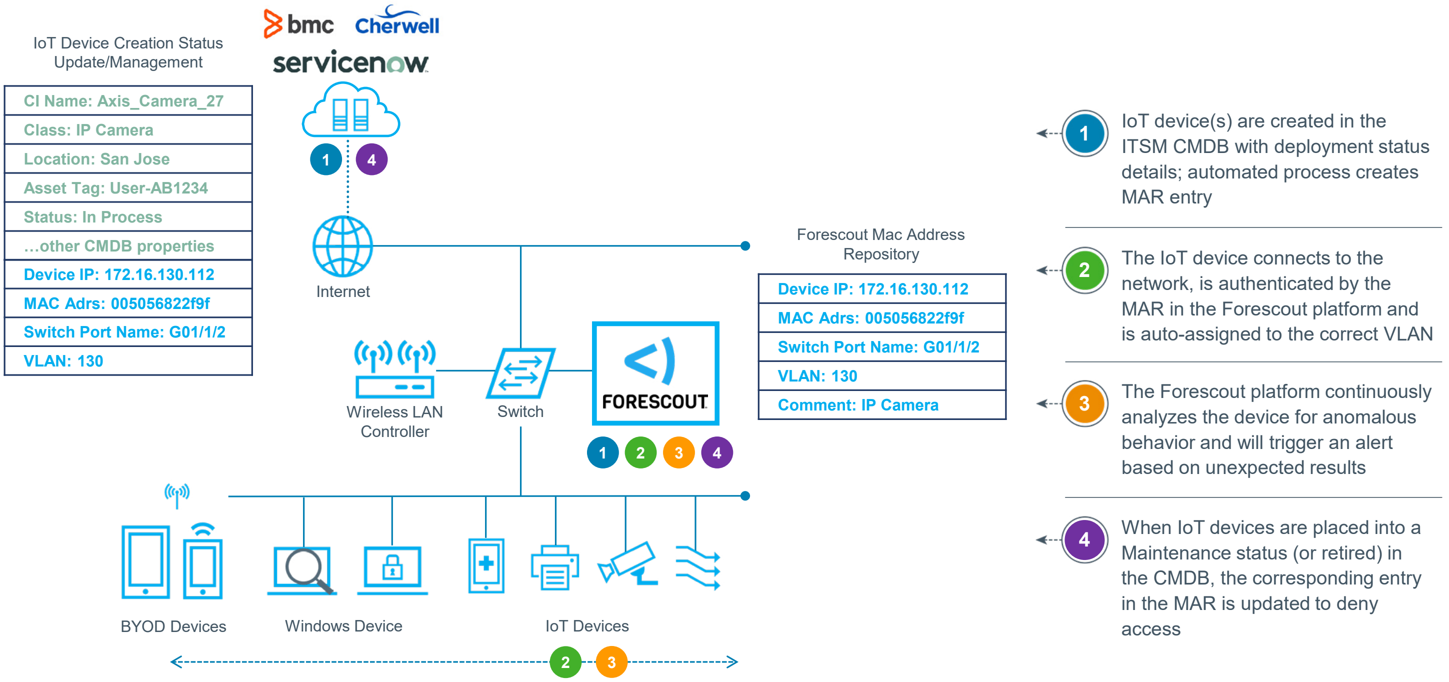
Automation of MAR for IoT Authentications

Devices are added to the CMDB as part of the asset management lifecycle. However, IoT devices do not support supplicants (agents) as part of an 802.1X-based network authentication strategy and require some administration to ensure they are placed in the correct VLAN and that they continue to act without anomalous behavior. As their deployment status changes during the onboarding process, IoT devices are automatically added to the Forescout platform MAR with the appropriate network access privileges based on what is configured in the Forescout platform.

- Each of the various types of devices are automatically placed into the correct VLANs based on their type as prescribed in the MAR.
- Additional device behavior analysis compared against the assigned VLAN based on the CMDB entry provides defenses against MAC spoofing.
- When devices are taken offline for maintenance or retired permanently, the entry in the CMDB is updated with an accompanying status that is sent to the Forescout platform MAR with deny settings that ensure they are not granted access.

Workflow

1. The device status is updated in the CMDB and the ITSM platform creates/updates an entry in the Forescout platform MAR.
2. The device connects and is automatically assigned to the correct VLAN with the appropriate settings as set forth by the MAR entry configuration.
3. When the device displays unexpected behavior, incidents can be created in the ITSM platform.
4. When the device is retired or placed into maintenance mode in the CMDB, access is automatically set to Deny in the MAR.



IoT Device Creation Status Update/Management

CI Name: Axis_Camera_27
Class: IP Camera
Location: San Jose
Asset Tag: User-AB1234
Status: In Process
...other CMDB properties
Device IP: 172.16.130.112
MAC Adrs: 005056822f9f
Switch Port Name: G01/1/2
VLAN: 130

Forescout Mac Address Repository

Device IP: 172.16.130.112
MAC Adrs: 005056822f9f
Switch Port Name: G01/1/2
VLAN: 130
Comment: IP Camera

1 IoT device(s) are created in the ITSM CMDB with deployment status details; automated process creates MAR entry

2 The IoT device connects to the network, is authenticated by the MAR in the Forescout platform and is auto-assigned to the correct VLAN

3 The Forescout platform continuously analyzes the device for anomalous behavior and will trigger an alert based on unexpected results

4 When IoT devices are placed into a Maintenance status (or retired) in the CMDB, the corresponding entry in the MAR is updated to deny access

Figure 5: Workflow: Automation of MAR for IoT authentication .

Use CMDB as the Verification Source for Authentications

In non-802.1X deployments, the Forescout solution ensures that all owned and/or authorized devices are in the CMDB. When devices attempt to connect to the network, the Forescout platform searches for the device in the CMDB. If the device is found with a valid status, the device is permitted onto the network.

Workflow

1. If the device doesn't exist in the CMDB, the Forescout platform sends discovered device details to the CMDB for authorized devices (e.g., domain member/managed devices, etc.)
2. When the device attempts to connect, the Forescout platform looks up the device's details and verifies its existence and status in the CMDB.
3. Upon successful verification, the device is granted access.
4. If needed, the CMDB is updated with new connection details or other attributes that may have changed.

Increase Service Desk Efficiency

The IT service desk function includes such processes as incident or problem management. The Forescout platform improves the efficiency and effectiveness of the service desk in the following ways:

- Ensuring that the CMDB is completely populated means more accurate incident tickets are created, driving down the mean time to resolution of issues
- Automating the intelligent ticketing process by initiating the creation of incidents based on events the Forescout platform solution has handled or received via third-party integration

Workflow

1. The Forescout platform user identifies an endpoint for which an IT incident must be created either through a policy or manually.
2. The Forescout platform user triggers a "Create IT Incident" action from the Forescout platform
3. An IT incident is added to the ITSM platform IT Incidents table, corresponding to the endpoint in the Forescout platform on which the Create IT Incident action was triggered.
4. The ITSM platform sends the incident number, category, subcategory, impact, urgency, priority, short description, and state updates back to the Forescout platform.
5. The ITSM platform user creates an action request to the Forescout platform.

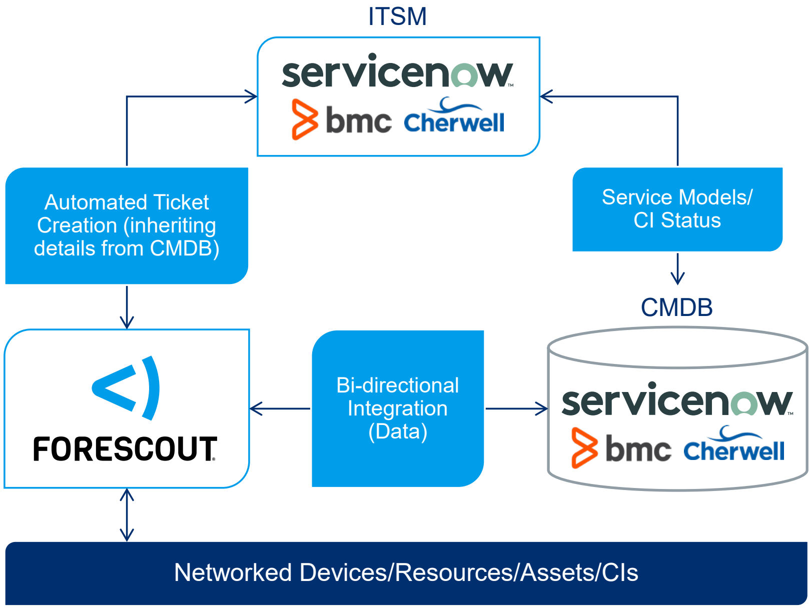

ITSM
servicenow
bmc Cherwell
Automated Ticket Creation (inheriting details from CMDB)
Service Models/ CI Status
CMDB
FORESCOUT
Bi-directional Integration (Data)
servicenow
bmc Cherwell
Networked Devices/Resources/Assets/CIs

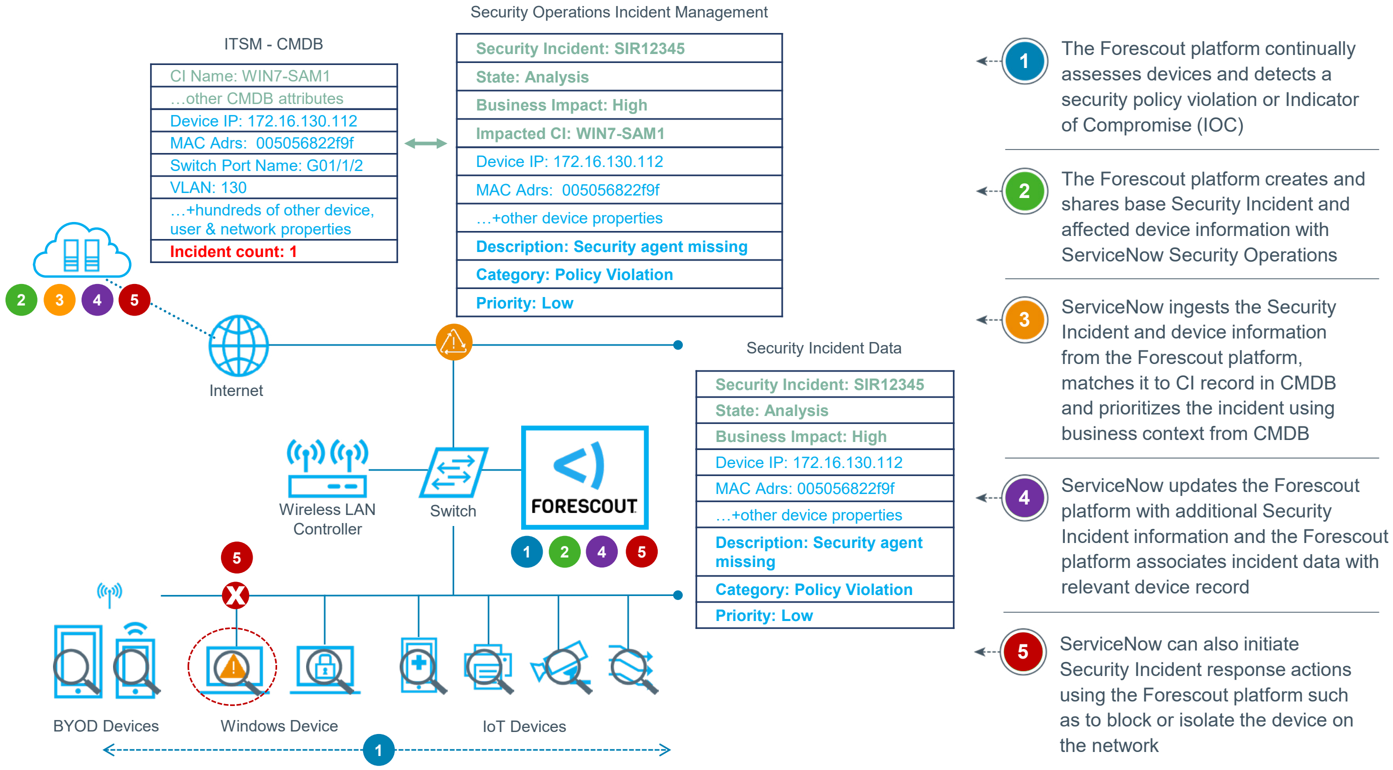
Figure 6: Workflow: how the Forescout platform improves service desk efficiency.

Optimize Security Operations

The Forescout platform is continuously analyzing the connected devices' security posture and can automatically create security incidents.

Workflow

1. The Forescout platform user identifies an asset for which a SOC incident must be created either through a policy or manually.
2. The Forescout platform user triggers a "Create SOC Incident" action from the Forescout platform.
3. A SOC incident is added to the ITSM platform Security Incidents table, corresponding to the endpoint in the Forescout platform on which the Create SOC Incident action was triggered.
4. The ITSM platform sends the incident number, category, subcategory, business impact, priority, short description, and state updates back to the Forescout platform.
5. The ITSM platform user creates an action request to the Forescout platform.



ITSM - CMDB

CI Name: WIN7-SAM1
…other CMDB attributes
Device IP: 172.16.130.112
MAC Adrs: 005056822f9f
Switch Port Name: G01/1/2
VLAN: 130
…+hundreds of other device, user & network properties
Incident count: 1

Security Operations Incident Management

Security Incident: SIR12345
State: Analysis
Business Impact: High
Impacted CI: WIN7-SAM1
Device IP: 172.16.130.112
MAC Adrs: 005056822f9f
…+other device properties
Description: Security agent missing
Category: Policy Violation
Priority: Low

Security Incident Data

Security Incident: SIR12345
State: Analysis
Business Impact: High
Device IP: 172.16.130.112
MAC Adrs: 005056822f9f
…+other device properties
Description: Security agent missing
Category: Policy Violation
Priority: Low

1 The Forescout platform continually assesses devices and detects a security policy violation or Indicator of Compromise (IOC)

2 The Forescout platform creates and shares base Security Incident and affected device information with ServiceNow Security Operations

3 ServiceNow ingests the Security Incident and device information from the Forescout platform, matches it to CI record in CMDB and prioritizes the incident using business context from CMDB

4 ServiceNow updates the Forescout platform with additional Security Incident information and the Forescout platform associates incident data with relevant device record

5 ServiceNow can also initiate Security Incident response actions using the Forescout platform such as to block or isolate the device on the network

Figure 7: Workflow: how the Forescout platform helps to optimize security operations.

Security Compliance

In order to accurately ascertain device compliance in a heterogeneous network environment, there first needs to be a full understanding of the assets deployed around the enterprise. Once the Forescout platform has visibility and management of the full population of network connected assets, reporting on compliance can easily be achieved, either via the inherent analytical capabilities the Forescout platform provides or via integration with third-party solutions such as Splunk. In any case, the completely populated CMDB ensures full compliance can be reported.

Workflow

1. The Forescout platform is continuously analyzing devices for compliance against established policies.
2. If configured to do so, the Forescout platform can initiate a network-based restriction to isolate the noncompliant device(s).
3. The Forescout platform automatically initiates a remediation of the device(s). That remediation may include patching or a script execution to remove an unauthorized application/file or reconfigure a system setting.
4. Then, after bringing the device to a point of compliance, the Forescout platform removes the restriction, allowing for normal usage.

Out of the box integration with ServiceNow

Forescout offers an out the box and fully supported bi-directional integration with ServiceNow that helps to provide all the use cases outlined above. The integration takes advantage of the unmatched asset identification and classification capabilities across traditional IT, OT and IoT domain areas.

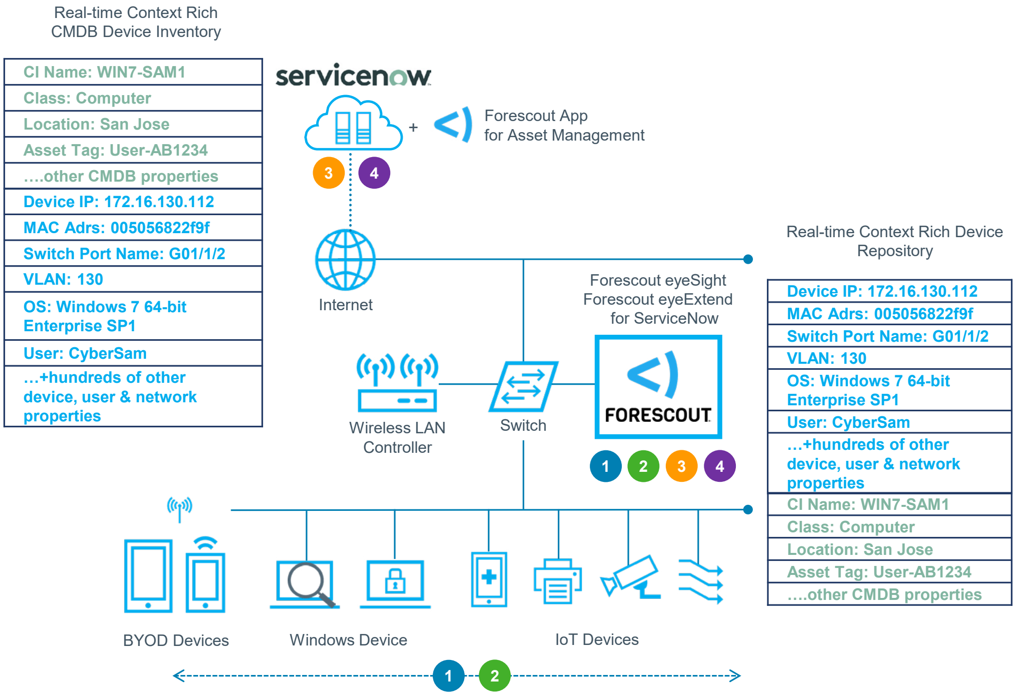
After the baseline configuration is established in the Forescout platform, synchronization into ServiceNow is easily achieved, which provides the basic asset data needed to support each of the use cases previously explained. Once the initial upload into ServiceNow has taken place, the Forescout platform can ensure that the data in the CMDB is kept updated. When installed into ServiceNow, the Forescout platform App for Asset Management creates a staging table. Forescout's solution uses that staging table as the intermediary landing area for the data uploads prior to scripts performing normalization and reconciliation activities.

Based on policy and adhering to the change-management policies, the Forescout platform uses a lookup key to match the device(s) and updates the selected properties as configured. The Forescout platform App for Asset Management supports integration between the Forescout platform and ServiceNow. The CMDB is enriched and supplemented by the bi-directional data exchange between the Forescout platform and ServiceNow. Through adding or updating of device properties on ServiceNow's CMDB configuration item tables, the Forescout platform triggers the ServiceNow workflow by applying the Forescout platform's policies. These policies are based on Forescout platform properties and the properties exchanged with the ServiceNow instance.

The data exchange is as follows:

1. Identify devices on network segments across IT and OT using the Forescout platform appliance(s)
2. Update ServiceNow tables with device properties captured by the Forescout platform.
3. Import device properties from ServiceNow of which the Forescout platform was not aware.

The Forescout platform App for Asset Management also includes tables, import sets and scripts needed by the Forescout platform App for IT Incidents and the Forescout platform App for SOC Incidents. These additional objects let the Forescout platform App for Asset Management push updates to the Forescout platform.



Real-time Context Rich CMDB Device Inventory
servicenow
+
Forescout App for Asset Management
3
4
Internet
Real-time Context Rich Device Repository
Forescout eyeSight Forescout eyeExtend for ServiceNow
Wireless LAN Controller
Switch
FORESCOUT
1
2
3
4
BYOD Devices
Windows Device
IoT Devices
1
2

Real-time Context Rich CMDB Device Inventory

CI Name: WIN7-SAM1
Class: Computer
Location: San Jose
Asset Tag: User-AB1234
….other CMDB properties
Device IP: 172.16.130.112
MAC Adrs: 005056822f9f
Switch Port Name: G01/1/2
VLAN: 130
OS: Windows 7 64-bit Enterprise SP1
User: CyberSam
…+hundreds of other device, user & network properties

Real-time Context Rich Device Repository

Device IP: 172.16.130.112
MAC Adrs: 005056822f9f
Switch Port Name: G01/1/2
VLAN: 130
OS: Windows 7 64-bit Enterprise SP1
User: CyberSam
…+hundreds of other device, user & network properties
CI Name: WIN7-SAM1
Class: Computer
Location: San Jose
Asset Tag: User-AB1234
….other CMDB properties

1 The Forescout platform discovers, classifies and assesses all IP-connected device types as they connect to the network

2 The Forescout platform updates its asset repository with real-time hardware and software information

3 The Forescout platform then updates or creates a new ServiceNow® CMDB Configuration Item (CI) with device properties and additional network context from the Forescout device repository to true-up the CMDB and establish a real-time as well as historical single-source-of-truth for all assets

4 The Forescout platform imports device properties from ServiceNow that can be used to refine the Forescout platform enforcement policies and actions

Figure 8: Workflow: how the Forescout platform interacts with ServiceNow to update and maintain both Forescout platform and ServiceNow device intelligence.

The Forescout Platform and Other ITSM Solutions

In addition to ServiceNow, there are multiple ITSM solutions in the marketplace, namely BMC Helix (formerly Remedy) and Cherwell Service Management, among others. The same foundational data that the Forescout platform manages and synchronizes with ServiceNow can also be provided to those other solutions as well Forescout-provided integrations. This ensures that, regardless of the existing enterprise ITSM solution, the CMDB can be accurately populated to support the accompanying ITSM processes and applications.

Depending on the integration capabilities of the ITSM solutions themselves, the method of integration, as well as the functionality, what the Forescout platform is capable of will vary. Customers can leverage the Forescout platform's out-of-the-box and fully supported integration with ServiceNow that is pre-built to efficiently address everyday use cases. For other ITSM solutions, customers can either build or leverage community-built apps to integrate with the Forescout platform.

Product Requirements

Capability	Required Forescout Apps in ServiceNow Store (included as part of eyeExtend for ServiceNow license)	ServiceNow Product
Real-time asset intelligence and automatic CMDB update	Forescout App for Asset Management	Configuration Management Database
IT service incident creation and incident response	Forescout App for IT Incidents	IT Service Management
Security incident creation and incident response	Forescout App for Security Operations	Security Operations

Please note:

1. Forescout eyeSight is the base product required for all use cases
2. Forescout eyeControl is an add-on product required to facilitate Forescout platform actions for asset authentication and incident response
3. Forescout eyeExtend for ServiceNow is a required product to orchestrate workflows between the Forescout platform and ServiceNow
4. Forescout eyeExtend Connect product is used to create custom integrations for orchestrating workflows between the Forescout platform and other ITSM platforms

Learn More: https://www.forescout.com/partners/technology-partners/servicenow/

References

[1] Microsoft Endpoint Configuration Manager (Configuration Manager, also known as ConfigMgr or SCCM) is a systems management software product developed by Microsoft for managing large groups of computers running Windows NT, Windows Embedded, macOS (OS X), Linux or UNIX, as well as Windows Phone, Symbian, iOS and Android mobile operating systems. Source: https://en.wikipedia.org/wiki/Microsoft_System_Center_Configuration_Manager

[2] Simple Network Management Protocol (SNMP) is an Internet Standard protocol for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behavior. Source: https://en.wikipedia.org/wiki/Simple_Network_Management_Protocol

[3] A virtual LAN (VLAN) is any broadcast domain that is partitioned and isolated in a computer network.

[4] 802.1X is an IEEE Standard for port-based Network Access Control (PNAC). It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN.

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591

Learn more at forescout.com/partners/technology-partners/servicenow/